

## SECURITY & GOVERNANCE ON MICROSOFT FABRIC

Secure OneLake. Govern access. Enable trusted analytics at scale.

Quadrant's structured governance and security framework ensures Microsoft Fabric environments remain secure, compliant, and well-governed helping enterprises transform data into trusted AI-driven intelligence.



## QUADRANT GOVERNANCE & SECURITY FRAMEWORK

A four-pillar operating model to discover, govern, protect, and secure enterprise data in Microsoft Fabric

Trusted • Governed • Protected • Secure



### DISCOVER

Help users find the right trusted data product quickly.

#### Core capabilities

Catalog, search, and discovery

Domains and business context



### CONTROL

Govern access cleanly across workspaces, items, and personas.

#### Core capabilities

Workspace roles and item sharing

Least-privilege access model



### PROTECT

Limit data exposure with fine-grained business-aligned security.

#### Core capabilities

Sensitivity labels and classification

RLS/ OLS / CLS



### SECURE

Operate with visibility, auditability, and enterprise confidence.

#### Core capabilities

Audit, monitoring, and observability

Compliance and activity tracking

#### Microsoft Fabric Unified Data Estate

OneLake

Data Engineering

Data Warehouse

Real-Time Intelligence

Semantic Models

AI / Agents

## DEPLOYMENT APPROACH (2-6 WEEKS)

Assessment

Foundation

Guardrails

Operationalize

Scale



**Let's connect to drive innovation together.**

Build a secure, compliant, and well governed Microsoft Fabric environment with Quadrant's proven governance and security framework.